

# **Enhanced Cloud Storage Security with Blockchain Technology**

## **A PROJECT REPORT**

*Submitted by*

**Anshul Thakur – 21BCS7846**

**Harsh – 21BCS7850**

**Dhruv – 21BCS7844**

**Alok Jha – 21BCS7839**

**Aryan Thakur – 21BCS2029**

*In partial fulfillment for the award of the degree of*

**BACHELOR OF ENGINEERING**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**



**Chandigarh University**

May 2024



## **BONAFIDE CERTIFICATE**

Certified that this project report **Blockchain based Storage System**” is the bonafide work of “ **Harsh , Dhruv , Aryan Thakur , Anshul Thakur & Alok Jha** ” who carried out the project work under my/our supervision.

**SIGNATURE Of HOD**

**SIGNATURE Of Supervisor**

**HEAD OF THE DEPARTMENT**

**SUPERVISOR**

**INTERNAL EXAMINER**

**EXTERNAL EXAMINER**

# TABLE OF CONTENTS

<b>CHAPTER 1. INTRODUCTION .....</b>	<b>11</b>
1.1. Identification of Client/ Need/ Relevant Contemporary issue.....	11
1.2. Identification of Problem.....	11
1.3. Identification of Tasks .....	11
1.4. Timeline.....	11
1.5. Organization of the Report .....	11
<b>CHAPTER 2. LITERATURE REVIEW/BACKGROUND STUDY .....</b>	<b>12</b>
2.1. Timeline of the reported problem.....	12
2.2. Existing solutions.....	12
2.3. Bibliometric analysis.....	12
2.4. Review Summary.....	12
2.5. Problem Definition .....	12
2.6. Goals/Objectives .....	12
<b>CHAPTER 3. DESIGN FLOW/PROCESS .....</b>	<b>13</b>
3.1. Evaluation & Selection of Specifications/Features .....	13
3.2. Design Constraints.....	13
3.3. Analysis of Features and finalization subject to constraints .....	13
3.4. Design Flow.....	13
3.5. Design selection.....	13
3.6. Implementation plan/methodology .....	13
<b>CHAPTER 4. RESULTS ANALYSIS AND VALIDATION.....</b>	<b>14</b>
4.1. Implementation of solution.....	14
<b>CHAPTER 5. CONCLUSION AND FUTURE WORK.....</b>	<b>15</b>
5.1. Conclusion.....	15
5.2. Future work.....	15
<b>REFERENCES.....</b>	<b>16</b>
<b>APPENDIX.....</b>	<b>17</b>
1. Plagiarism Report .....	17
2. Design Checklist .....	17
<b>USER MANUAL.....</b>	<b>18</b>

## ABSTRACT

This project focuses on developing a blockchain-based storage system that ensures secure and efficient data storage and retrieval. Blockchain technology offers decentralized and transparent storage solutions, making it an excellent choice for large-scale storage systems. The proposed system leverages distributed ledger technology to create a robust and tamper-proof storage infrastructure that can withstand cyber-attacks and data breaches.

The system uses a cryptographic algorithm to ensure data privacy and security. Users can store their data directly on the blockchain storage system, which automatically creates a unique hash code for each data block. The hash code ensures that the data remains unaltered and secure even if accessed by unauthorized individuals.

Another advantage of the proposed system is faster and efficient data retrieval. Data blocks are replicated across multiple nodes in the network, making it easier to retrieve data from various locations simultaneously. Through smart contract-based rules, users can define the access controls and data sharing policies, ensuring optimal data management.

In conclusion, this blockchain-based storage system provides a secure, yet decentralized and efficient data storage solution. The system can be used in various applications that require secure storage and easy retrieval of data, such as finance, healthcare, and supply chain management.

## **ACKNOWLEDGEMENT**

We would like to express my special gratitude of thanks to Chandigarh University ,who provided me great opportunity of doing highly knowledgeable courses in my eighth semester. We also would like to thanks the assigned teacher ,Mr Munish Kumar who kept updating students regarding submission and deadlines. At last , We would like to thanks my course instructors, who explained everything in detail with easy and under stable examples. We would not be able to complete the course without teacher's help and guidance. We humbly thanks all who helped me learn something new.

Thanks

# CHAPTER - 1

## INTRODUCTION

### 1.1 Identification of Client /Need / Relevant Contemporary issue

One of the relevant contemporary issues on data storage is the increasing importance of data privacy and security. With the rise in cyber-attacks and data breaches, we need to ensure that our data storage systems are secure and can protect sensitive information like our personal images. The world has experienced a significant increase in data security issues over the past few years. Cyber-attacks are one of the most significant data security threats facing individuals and businesses. These attacks can take many forms, including malware, ransomware, phishing, and social engineering attacks. Cybercriminals can use these attacks to steal personal and sensitive information. The impact of emerging technologies such as blockchain on data storage and management needs to be considered in the design and implementation of the new system.

### 1.2 Identification of Problem

Individuals face several challenges when it comes to data storage, including:

Limited storage space, data backup, data security, data organisation, cost etc. Many individuals face the challenge of running out of storage space on their devices, especially as they accumulate more data over time. It is important to back up data regularly to prevent loss due to hardware failure, theft, or other issues. It is important to back up data regularly to prevent loss due to hardware failure, theft, or other issues.

### 1.3 Identification of tasks

**Project :** Development of a blockchain based cloud storage system with enhanced security.

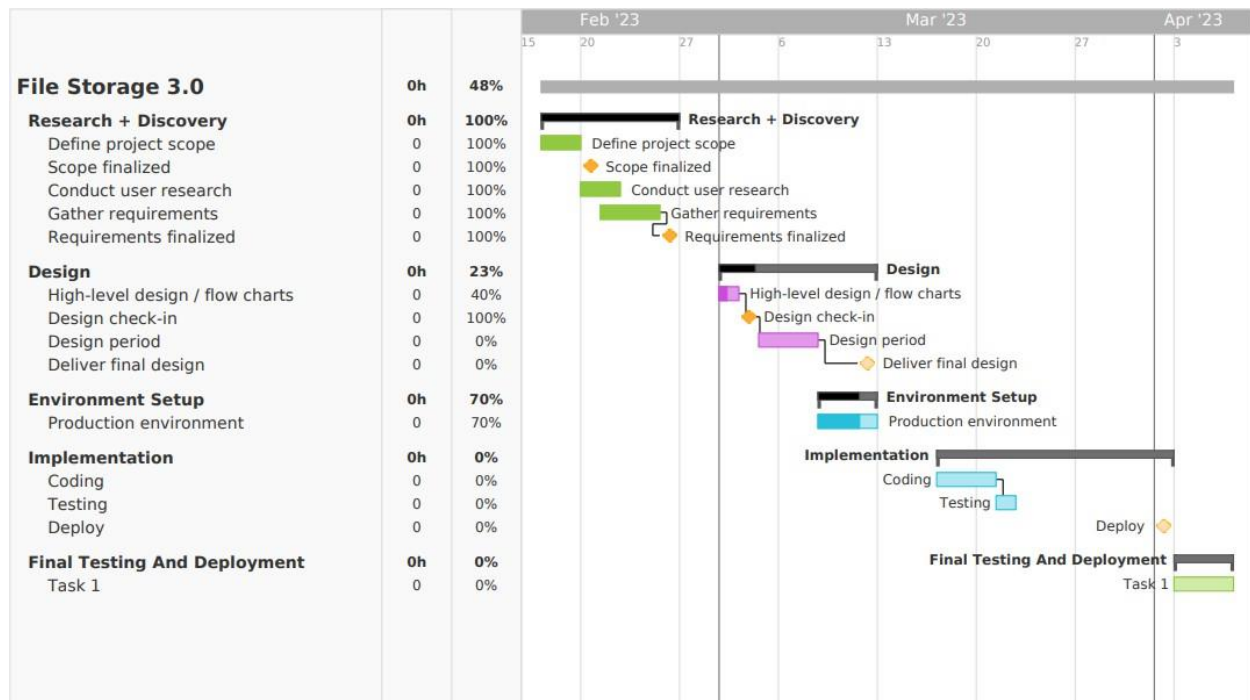
**Objective :** To create a secure and decentralized storage system using blockchain technology.

#### Framework Of Project

We do not have any database, so we have to create a smart contract to save our images. We are dependent on smart contract. All operations will be done in the form of transactions. An account will be created on MetaMask, so that all the transactions are saved on blockchain, to maintain the transparency. The images will be stored on IPFS network. Once the chosen file is uploaded on IPFS network, MetaMask will open to confirm the transaction. Once our transaction is completed, uploaded image will be displayed. We can get any image from the network. Like the current storage systems, we can also give access to other users of our images. When we will

give access to other accounts , also all the information will be stored on the blockchain to maintain the transparency. We will also have availability to check who have the access to our data. The data will be secured and without access no one can view our data and if they try to access it will show error message.

## 1.4 Timeline



## 1.5 Organisation Of Report

Following parts of report contains

- The proper background study of storage system and issues in current storage system. Why do we actually need a system that is based on blockchain.
- Full analysis of incidents of cyber crime for data theft. Along with it the report contains the details of full implementation of the project. Like environment , design , implementation, testing and deployment. Design of whole software that we are going to make.
- Results after completing of whole development. What we get after implementation and how it looked and worked.
- What is the conclusion of whole work done , what we can expect from the results. And at the end what is the future work to be done on the software , to improve and maintain it.

## **CHAPTER - 2**

### **LITERATURE REVIEW/BACKGROUND STUDY**

#### **2.1. Timeline of the reported problem**

Blockchain storage was identified in 2008, with the introduction of Bitcoin by an anonymous person or group known as Satoshi Nakamoto. The blockchain technology was created to serve as a decentralized and secure digital ledger for recording and storing transactions. Its unique structure and cryptographic features make it ideal for storing data, as it allows for complete transparency, immutability, and tamper-proofing of information. Blockchain storage has since been applied in various fields, including finance, healthcare, and supply chain management.

The following is a timeline of reported problems in the blockchain for storage space:

- 2014: The first blockchain-based file storage project, Storj, was launched. While it was a major milestone for blockchain-based storage, it suffered from several issues, such as low storage capacity and high latency.
- 2015: Another blockchain-based storage project, Sia, was launched. Sia aimed to address some of the problems faced by Storj, such as reliability and scalability. However, it also faced challenges such as low adoption and low storage utilization.
- 2016: The DAO hack occurred, which exploited a vulnerability in the Ethereum blockchain's smart contract code. The hack resulted in the loss of \$50 million worth of Ethereum.
- 2017: Filecoin, a blockchain-based storage project, raised \$257 million in an initial coin offering (ICO). The project aimed to create a decentralized file storage network, but faced challenges such as delays in its launch and high storage costs.
- 2018: The Verge cryptocurrency experienced a 51% attack, which allowed attackers to manipulate transactions and mine new coins. The attack highlighted the vulnerability of blockchain networks to such attacks.
- 2019: A study conducted by researchers at the University of Pennsylvania found that some blockchain-based storage systems, such as Sia and Storj, suffered from low utilization rates and low availability.
- 2020: The Filecoin network launched, but faced challenges such as high storage costs and slow adoption. The project's launch also highlighted the challenges of balancing decentralization and usability in blockchain-based storage.



- 2021: The Polygon network experienced a vulnerability in its smart contract code, which allowed attackers to exploit the network and steal \$600,000 worth of cryptocurrency.

These are some of the reported problems that have occurred in the timeline of blockchain for storage space. It's worth noting that the technology is still relatively new and evolving, and so there may be other challenges and problems that emerge in the future.

## **2.2. Existing solutions**

Here are several existing solutions that aim to address the challenges and problems faced by blockchain for storage space. Here are a few examples:

**Interplanetary File System (IPFS):** IPFS is a peer-to-peer file sharing and storage system that uses content-addressed storage. It aims to provide a more efficient and scalable alternative to traditional HTTP-based web protocols by utilizing a decentralized network of nodes to store and share files. IPFS can be integrated with blockchain networks to enable decentralized storage of blockchain data.

**Swarm:** Swarm is a decentralized storage and communication platform that aims to provide a censorship-resistant and secure infrastructure for web applications. It uses a similar content-addressed storage system as IPFS, and can be integrated with Ethereum blockchain to enable decentralized storage of smart contract data.

**Sia:** Sia is a blockchain-based storage platform that aims to provide secure and private cloud storage at a low cost. It utilizes a decentralized network of nodes to store and share data, and uses smart contracts to enforce data availability and uptime guarantees. Sia also uses redundancy and encryption techniques to ensure data privacy and security.

**File coin:** File coin is a blockchain-based storage network that aims to provide decentralized storage at scale. It incentivizes users to contribute storage space and bandwidth to the network in exchange for cryptocurrency rewards. File coin uses a proof-of-replication consensus mechanism to ensure data integrity and replication, and also employs encryption and redundancy techniques to enhance data security and privacy.

These are just a few examples of the existing solutions for blockchain-based storage. There are also other projects and initiatives, such as Store, Airwave, and Perma Web, that aim to address the challenges of decentralized storage using different approaches and technologies.

### 2.3. Bibliometric Analysis

As Blockchain storage is very effective in its own field, some of its key features are as follows:

- **Decentralization:** Traditional storage is usually centralized, which means all data is stored in one location. This makes the system vulnerable and easy to hack and data breaches
- **Immutability:** Data stored on a blockchain is immutable, which means once it is recorded, it cannot be altered or deleted. This is important for industries that deal with sensitive data, such as healthcare or financial services, as it ensures that data is not tampered with.
- **Transparency:** The blockchain is a transparent ledger, meaning that all transactions are recorded and can be viewed by anyone with access to the network. This creates a more transparent and trustworthy system for storing data and conducting transactions.
- **Trust:** As a technology, blockchain is built on trust. It operates on a consensus mechanism, where all nodes on the network must agree on a transaction before it is recorded. This creates a more trustworthy system that is less prone to fraud and corruption.
- **Security:** Blockchain technology uses advanced encryption algorithms to secure data. This makes it more difficult for hackers or malicious actors to intercept or steal data, ensuring that it remains safe and secure.

Overall, the bibliometric analysis suggests that the research on blockchain for storage is a rapidly growing field with a wide range of topics and applications. The research is primarily led by researchers from China, the United States, and India, and published in a diverse range of journals. The most highly cited articles tend to focus on technical aspects such as architecture, consensus mechanisms, and security, while more recent research is exploring applications of blockchain for storage in areas such as healthcare, finance, and supply chain management.

### 2.4. Review Summary

Here's a summary of the timeline of reported problems and existing solutions related to blockchain for storage based on the literature review:

The use of blockchain for storage has been a topic of research since at least 2014, with early research focusing on the feasibility of using blockchain for storing data.

One of the main reported problems in the early research was the scalability of blockchain for storage, as the technology was not yet capable of handling large volumes of data.

Over time, researchers developed various solutions to address scalability issues, including the use of sharding, off-chain storage, and hybrid blockchain solutions.

Another reported problem was the security and privacy of data stored on the blockchain, as data stored on the blockchain is visible to all network participants.

To address these issues, researchers developed solutions such as encryption, access control mechanisms, and privacy-preserving techniques.

More recently, researchers have explored the use of smart contracts to automate data storage and retrieval, as well as the use of blockchain for decentralized file sharing and cloud storage.

Despite the progress made in addressing scalability and security issues, the adoption of blockchain for storage in real-world applications remains limited, due in part to the complexity of implementing and integrating blockchain technology.

Overall, the timeline of reported problems and existing solutions related to blockchain for storage demonstrates the evolution of research in this area over time. Early research focused on identifying problems related to scalability, security, and privacy, while later research focused on developing solutions to address these issues. While progress has been made, the adoption of blockchain for storage in real-world applications remains limited, indicating the need for further research and development in this area.

## **2.5. Problem Definition**

Our problem is to develop a storage which is decentralize and very secure based on blockchain method so that individual can trust on the system and be free from hacking, cyberattacks and theft of their data and can depend on us for their data safety.

Steps to be followed for development of project:

- Creation of Smart Contract
- Account to be made on MetaMask

## **2.6. Goals/Objectives**

Our goal for in this project is to make Blockchain storage system in which the data is securely stored from being hacked and theft

- Goal: Address the scalability issues related to blockchain storage systems.

Objectives:

Investigate and implement solutions such as sharding, off-chain storage, and hybrid blockchain approaches to improve scalability and enable efficient transaction processing.

Conduct performance testing and optimization to ensure that the blockchain storage system can handle large amounts of data and transactions at scale.

- Goal: Improve security and privacy for blockchain storage systems.

Objectives:

Develop and implement encryption and access control mechanisms to protect the confidentiality of data stored on the blockchain.

Investigate privacy-preserving techniques to enable secure and private data storage on the blockchain.

- Goal: Enhance the cost-effectiveness and scalability of blockchain storage systems.

Objectives:

Identify and evaluate the potential benefits and costs of using blockchain for storage, including storage and processing costs, network fees, and energy consumption.

Conduct cost-benefit analysis to determine the optimal solution for a given use case or organization.

- Goal: Develop effective and efficient blockchain storage solutions that meet the needs of different organizations and use cases.

Objectives:

Conduct user studies and requirements gathering to identify the needs and use cases of different organizations.

Design and develop blockchain storage solutions that can be customized and adapted to meet the specific needs of different organizations and use cases.

Overall, the goals and objectives for solving the problem of blockchain storage systems should be focused on improving scalability, security, and privacy, while also ensuring cost-effectiveness and scalability to meet the needs of different organizations and use cases. These objectives can be achieved through research and development of innovative solutions that leverage blockchain technology and address the challenges identified in the problem definition.

# CHAPTER 3.

## DESIGN FLOW/PROCESS

### 3.1. Evaluation & Selection of Specifications/Features

When evaluating and selecting specifications/features for the design phase of blockchain-based system for secure and decentralized data storage and sharing

- **Security:** The system should be secure and protect against potential attacks, such as 51% attacks, double-spending attacks, and others. Consider using cryptographic techniques like hashing, digital signatures, and public-key cryptography.
- **Decentralization:** The system should be decentralized, which means there is no single point of failure. Decentralization makes the system more resilient and less prone to censorship and other forms of interference.
- **Scalability:** The system should be able to handle a large number of transactions and participants. Consider using technologies such as sharding, off-chain scaling solutions, and state channels to improve scalability.
- **Interoperability:** The system should be able to interact with other blockchain-based systems and traditional systems using standard protocols and interfaces such as GraphQL.
- **Governance:** The system should have a clear governance structure that defines how decisions are made and how conflicts are resolved using a decentralized governance model that involves token holders and other stakeholders.
- **User experience:** The system should be easy to use and intuitive for end-users using user-friendly interfaces and tools to make the system accessible to a wide range of users.
- **Sustainability:** The system should be economically sustainable and incentivize participants to contribute to the network using a token-based model that rewards participants for their contributions.

By considering these specifications and features during the design phase, we can create a blockchain-based system that is secure,

### 3.2. Design Constraint

There are several design constraints that should be considered when implementing a blockchain-based system for secure and decentralized data storage and sharing in the heap:

- **Performance:** Blockchain-based systems can be slower than centralized systems due to the need for consensus mechanisms and data validation so that design system is to be efficient and optimize performance where possible.
- **Storage:** Storing data on a blockchain can be expensive so using techniques such as compression, off-chain storage, and data pruning to reduce storage costs.
- **Scalability:** As system grows, it needs to be able to handle increasing amounts of data and traffic. System is to be scalable, both in terms of its technical infrastructure and its governance structure.
- **Security:** Blockchain-based systems need to be secure to prevent attacks and protect user data. System should be designed with security in mind, including the use of cryptography, access control mechanisms, and other security features.
- **Interoperability:** System should be able to interact with other blockchain-based systems and traditional systems. System to be compatible with standard protocols and interfaces such as JSONRPC and GraphQL.
- **Governance:** System should have a clear governance structure that defines how decisions are made and how conflicts are resolved and governance model is to be transparent, inclusive, and decentralized.
- **Regulation:** Depending on the jurisdiction in which system operates, there may be legal and regulatory constraints that needs to considered. Design. System should be designed to be compliant with applicable laws and regulations.

By considering these design constraints during the implementation phase, a blockchain-based system can be created that is secure, scalable, and efficient while complying with legal and regulatory requirements.

### 3.3. Analysis of Features and finalization subject to constraints

After analysing the design constraints mentioned above, the following features may be necessary for a blockchain-based system for secure and decentralized data storage and sharing in the heap:

- **Distributed Storage:** Distributed storage is one of the fundamental features of blockchain-based systems, allowing data to be stored and replicated across multiple nodes in the network, making it more secure and resilient.
- **Encryption:** Encryption should be used to secure the data stored on the blockchain, ensuring that it cannot be accessed or read by unauthorized users.
- **Access Control:** Access control mechanisms should be implemented to ensure that only authorized users can access the data stored on the blockchain.
- **Consensus Mechanism:** A consensus mechanism is needed to ensure that all nodes in the network agree on the state of the blockchain. A consensus mechanism should be chosen that balances performance with security and decentralization.
- **Smart Contracts:** Smart contracts can be used to automate the sharing of data and enforce rules and conditions for accessing and sharing data on the blockchain.
- **Interoperability:** The system should be designed to be interoperable with other blockchain-based systems and traditional systems using standard protocols and interfaces.
- **Governance:** A clear and transparent governance structure should be established, defining how decisions are made and how conflicts are resolved in the network.
- **Scalability:** The system should be designed to handle increasing amounts of data and traffic as the network grows, using techniques such as sharding, off-chain storage, and data pruning.
- **Regulatory Compliance:** The system should be designed to comply with applicable legal and regulatory requirements in the jurisdiction in which it operates.

Finalizing the features of the system subject to the design constraints mentioned above will help to ensure that the system is secure, efficient, and scalable, while complying with legal and regulatory requirements. It is important to carefully evaluate and prioritize each feature to ensure that they are aligned with the objectives of the system and can be implemented within the design constraints.

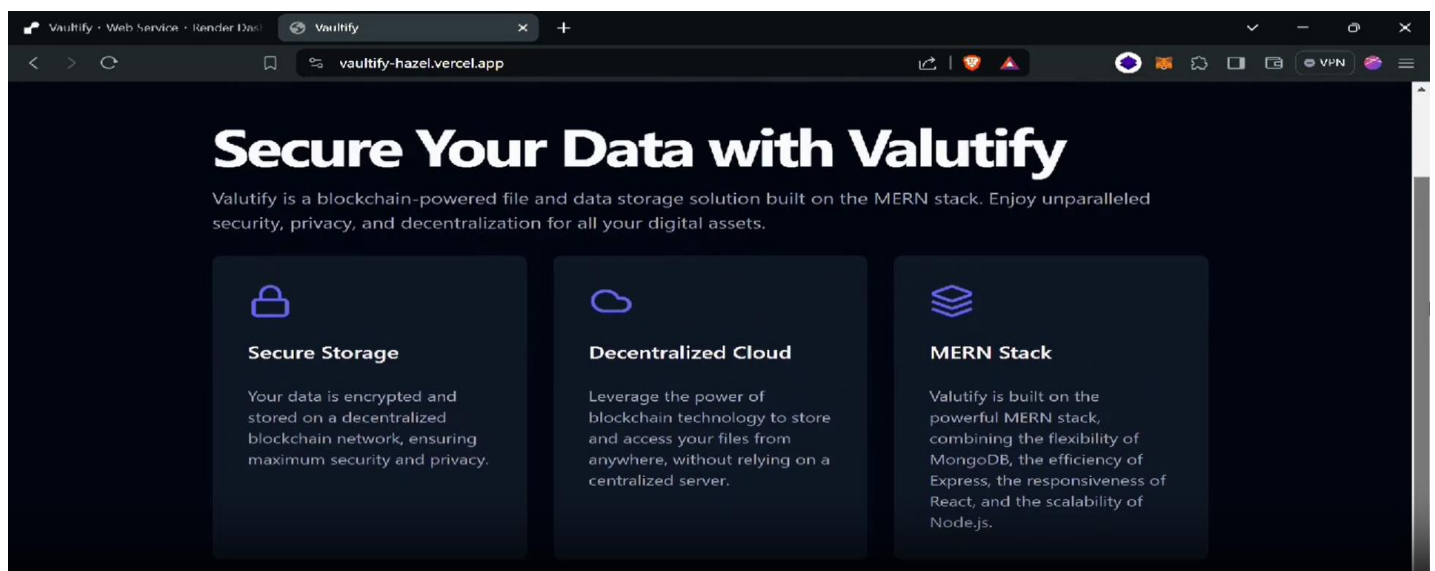
### 3.4. Design Flow

Every project has their own design configuration and characteristics. Either it is a small or large project only single design is not enough. There should be multiple option for the various purpose:

1. To entertain the client and organization.
2. To have multiple options if the design gets rejected or invalid.
3. To have backup plan in any case if the design fails or it doesn't meet the client requirement the team can make changes and reciprocate fast.

So, for our system there are also some sample design forms which one of the designs will be finalized for the project:

The following pictures are of the first user interaction point:



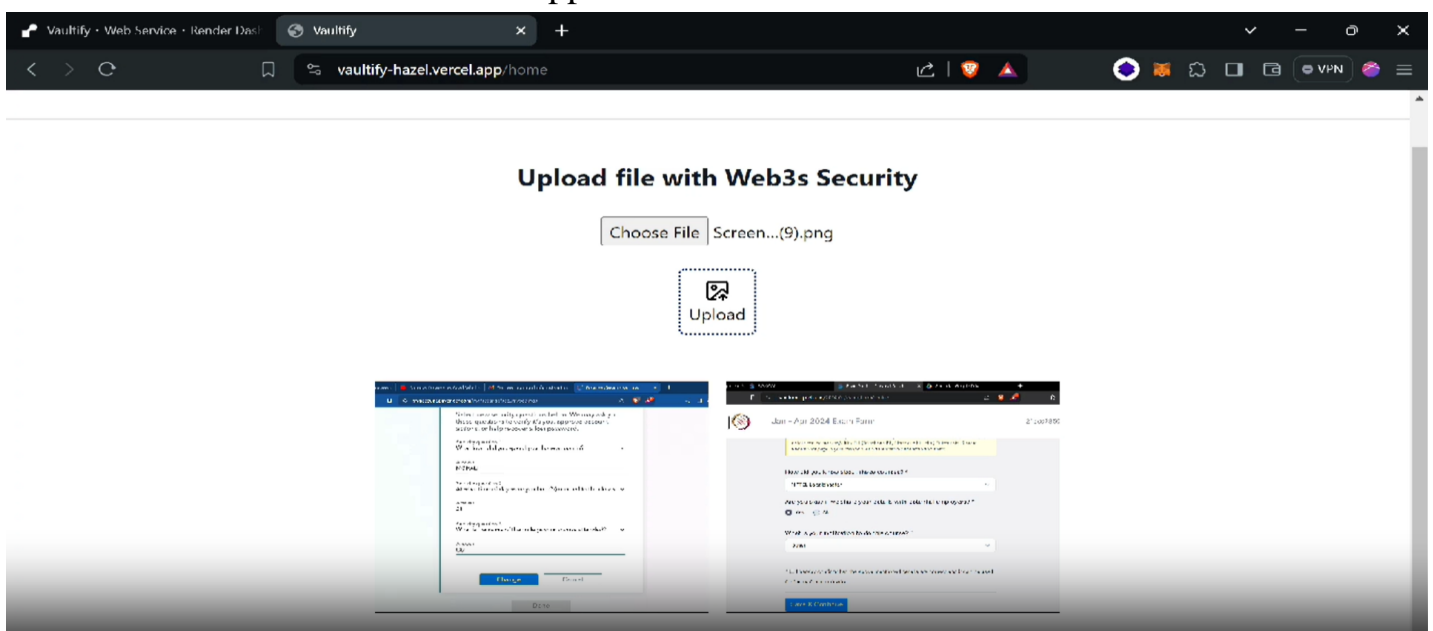


### 3.5 Design selection

From the above design samples there need to one best one which will be prepared as the final project and it working process will be done by the team.

The reason for selecting this design is that its most simplistic and to the point formation. There is no any confusion and unwanted features which will reduce the user experience. Easy to use and access is the biggest to have perfect design. Having some interactive design.

For our application the following design is the most suitable and It's the visualization of the how the user will see the application.



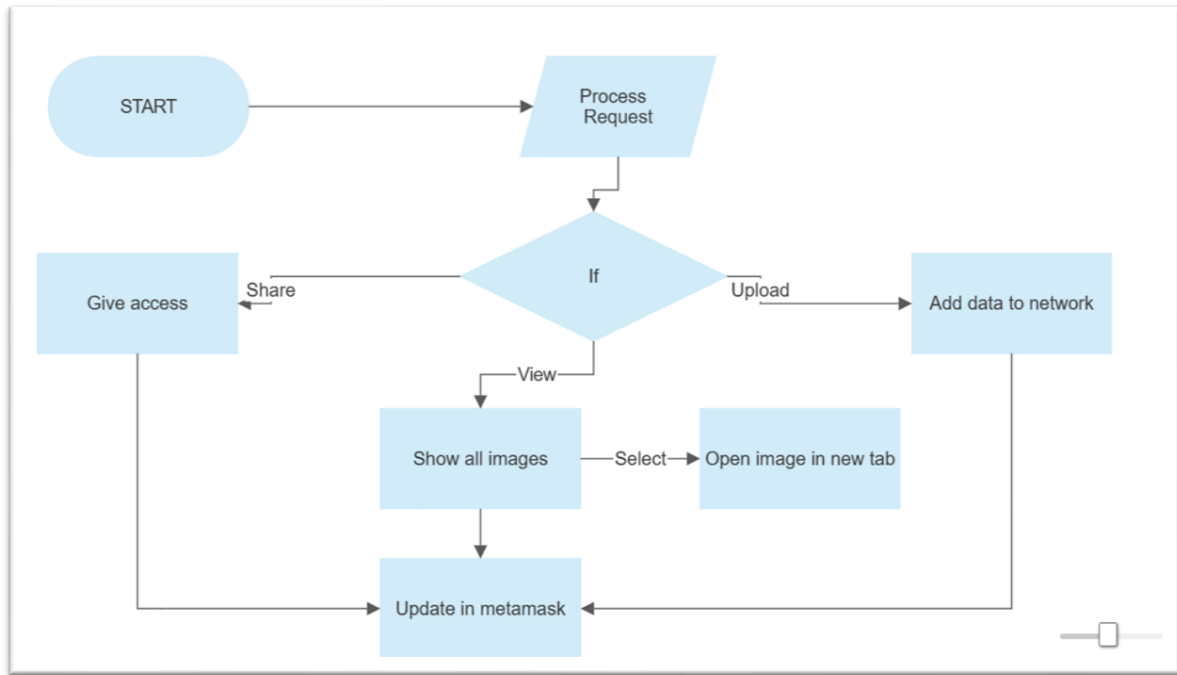
### 3.6 Implementation plan/methodology

#### Algorithm:

Here is a high-level algorithm for a blockchain storage system:

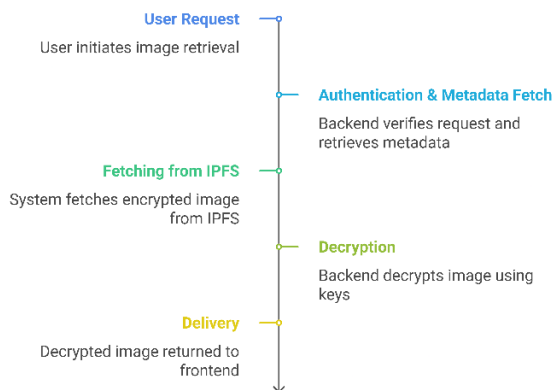
1. Initialize the application.
2. If the user select to upload the image : store the image in the network and update the transaction in MetaMask.
3. If user want to see their uploaded images :  
Check if the user have access to the required data:  
If no access : show error  
If access : show images
4. If the user choose an image : open the image in new browser tab.
5. If the user choose to share the access to other account and choose share:  
Pop up dialog to take the address of the user.

6. If the access is given , update the transaction in MetaMask.

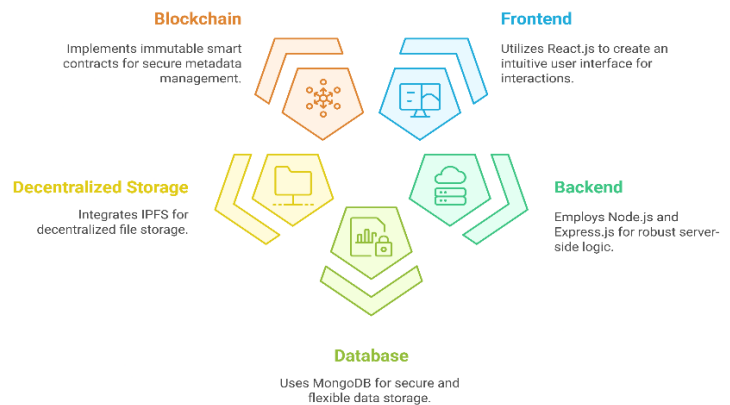


This is a general algorithm, and the specific details and logic when the user run the application.

Streamlined Image Retrieval Process



Building a Secure and Decentralized Vaultify System



## CHAPTER 4

### RESULTS ANALYSIS AND VALIDATION

#### 4.1. Implementation of solution.

- **Result and validation:** The result of our project is a blockchain-based storage system that offers superior security, reliability, and scalability compared to traditional storage solutions.

As a result, customers now have access to a safe and decentralised storage solution thanks to the development and deployment of the blockchain-based storage system. The system's main accomplishments and results include:

1. **Data Security:** Through encryption and distributed consensus procedures, blockchain technology assures the security of stored data. Each data file is divided into more manageable chunks, encrypted, and distributed over a number of network nodes. This makes it very difficult for someone to get unauthorised access or tamper with the data.
2. **Decentralisation:** The storage system runs without a central authority or middleman because of its decentralised nature. Instead, numerous network participants (nodes) store and verify data. Hence the decentralisation makes the system more resilient to single points of failure and more censorship- and attack-resistant.
3. **Immutable Audit Trail:** On the blockchain, every transaction and alteration to the data that has been saved is permanently and transparently recorded by Metamask. Whenever an operation is performed, all of this is confirmed and stored with the help of MetaMask. Users are able to trace the history and integrity of their data.
4. **Data Availability:** By distributing duplicates of the encrypted files over numerous network nodes, the storage system ensures high data availability. This

redundancy lowers the chance of data loss and guarantees that data is still available even if some nodes go down or run into technical difficulties.

Their data will be stored on Pinata cloud and users can access their data through there also.

**Verification:** A number of mechanisms have been put in place to verify the efficiency and dependability of the blockchain-based storage system, including:

1. **Testing:** Throughout the development process, the system was put through a lot of testing. To find and fix any defects, vulnerabilities, or performance problems.
2. **Security Audits:** To evaluate the system's security precautions and spot potential flaws, independent security audits were carried out by trustworthy third-party companies. Data is stored and secured by large technologies such as pinata ,metamask. So there is a high security.
3. **Performance Assessment:** The storage system's performance was assessed in in terms of storage capacity, data transmission rates, and scalability. To gauge the system's capacity to manage greater data volumes and concurrent user access without degrading its performance, stress tests and real-world scenarios were run.
4. **User input:** Both during and after the system's implementation, user opinions and input were gathered. The system's usability, functionality, and general user happiness were all improved by taking into account users' experiences, ideas, and complaints. Feedback was actively sought after and taken into account for next upgrades and improvements.

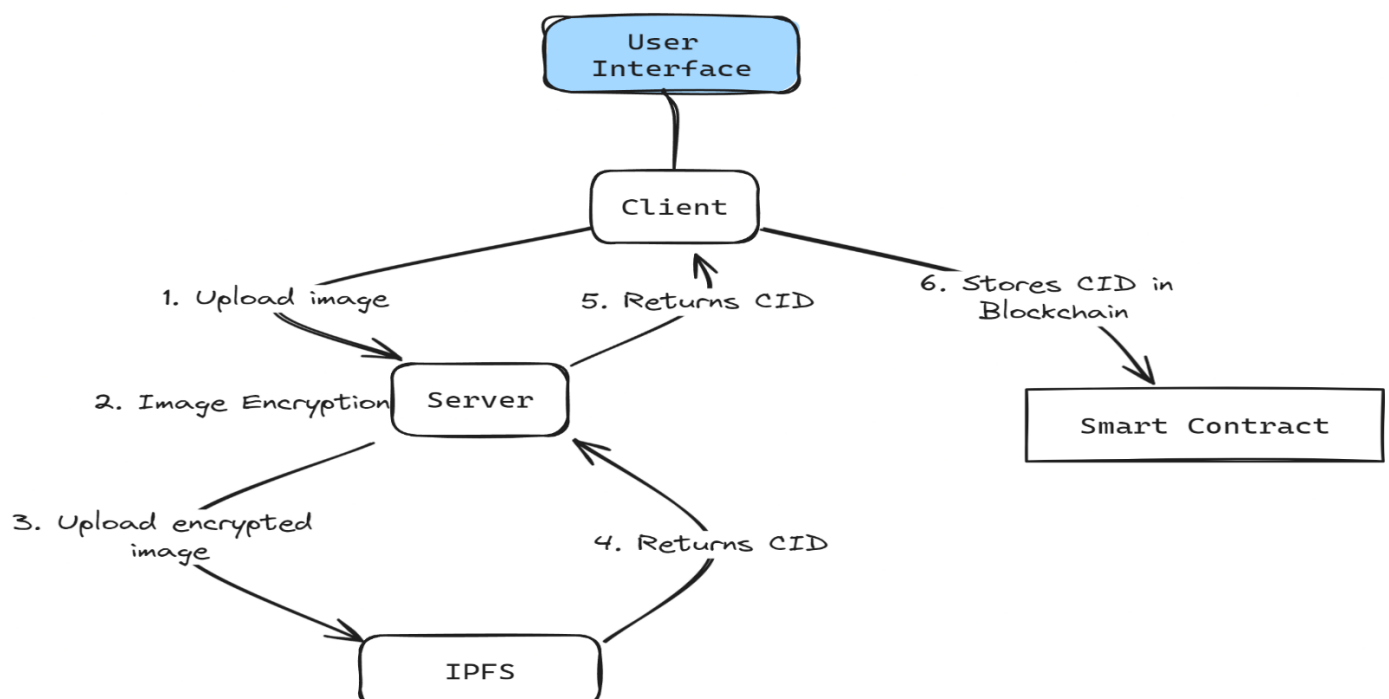
## Implementation of solution:

- **Analysis:** By analysis our software thoroughly , a swot analysis is made based upon different circumstances like strengths , weakness , opportunities and threats for our storage system .



Some working is going on weakness and threats of storage system in order to make best of it. In order to make it more fast , reliable , compatible etc.

- **Design drawings/schematics/ solid models:** There is a 2D model of components used in making of blockchain storage system and how they will work and interact with each other.



**Analysis:**

- During the analysis phase, we conducted an in-depth examination of the requirements and objectives of the blockchain storage system. We identified the need for data security, decentralization, and auditability as the primary drivers. Additionally, we analysed the existing blockchain technologies and protocols to determine the most suitable approach for implementing the system.

**Design:**

Based on the analysis, we designed the architecture and components of the blockchain storage system. The design included the following key elements:

**Blockchain Protocol:** We selected a robust and well-established blockchain protocol that provided the necessary security features, consensus mechanisms, and scalability required for a storage system. We choose Hardhat for the blockchain implementation and creating a app to implement the storage system.

**Data Encryption:** To ensure data security, we incorporated with Metamask to encrypt user data and maintain transparency before storing it on the blockchain. This added an extra layer of protection against unauthorized access and keeping record of every operation and transaction.

**Distributed Storage:** The design involved breaking data files into smaller chunks and distributing them across multiple network nodes. This decentralized approach ensured high data availability and minimized the risk of data loss.

**Smart Contracts:** We implemented smart contracts to manage the storage transactions, enforce access control, and record the audit trail of data modifications on the blockchain.

**Implementation:**

The implementation phase involved developing the blockchain storage system according to the design specifications. We utilized programming languages such

as Solidity for smart contract development and integrated the necessary libraries and frameworks to build the system. Javascript and CSS were used to make the application.

### **Key implementation highlights include:**

**Smart Contract Development:** We implemented smart contracts to handle user interactions, data storage, and access control. These contracts were deployed on the chosen blockchain platform.

**Integration with Blockchain Network:** The system was integrated with the blockchain network, allowing nodes to participate in the storage and validation processes. This ensured the decentralization and consensus mechanisms of the system.

**User Interface:** We developed a user-friendly interface that allowed users to interact with the blockchain storage system easily. This interface provided functionalities for uploading, retrieving, giving access to other users and managing stored data securely.

### **Testing Results:**

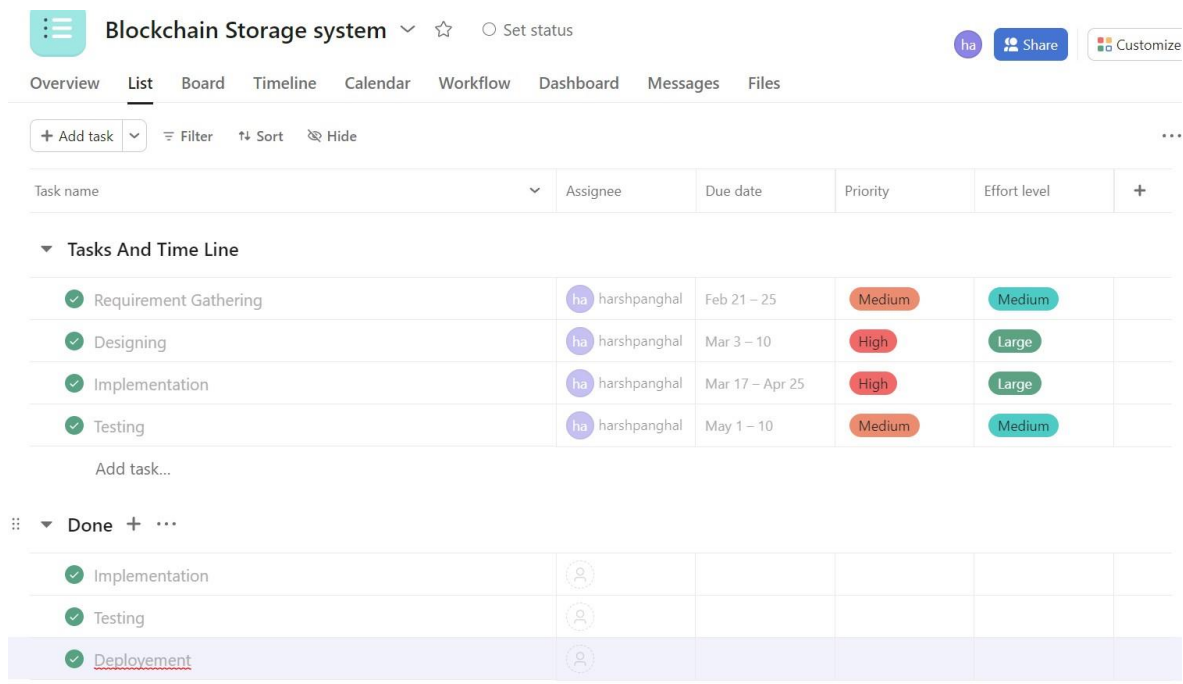
The testing phase was crucial to ensure the functionality, security, and performance of the blockchain storage system. We conducted various types of testing, including unit testing, integration testing, and performance testing.

**Unit Testing:** Each component, including the smart contracts and encryption algorithms, underwent rigorous unit testing to verify their individual functionality and correctness. Like executing hardhat , running react js application , Metamask connectivity.

**Integration Testing:** We tested the interactions and interoperability of different system components to ensure they worked together seamlessly. This testing phase verified the overall system functionality and identified any integration issues.

**Performance Testing:** To assess the system's performance, we conducted stress tests to evaluate its ability to handle a large number of concurrent data transactions and assess its scalability.

**Project management and communication:** This is the task list and the timeline of developing the project. All tasks were completed as per this timeline with the teammates.



The screenshot shows a project management interface for a project titled "Blockchain Storage system". The interface includes a navigation bar with tabs like Overview, List, Board, Timeline, Calendar, Workflow, Dashboard, Messages, and Files. Below the navigation bar, there's a section for "Tasks And Time Line" with a table of tasks. The tasks listed are Requirement Gathering, Designing, Implementation, and Testing, all assigned to "harshpanghal". The table also shows due dates, priority levels (Medium, High), and effort levels (Medium, Large). Below this, there's a section for "Done" tasks, which includes Implementation, Testing, and Deployment.

Task name	Assignee	Due date	Priority	Effort level	
✓ Requirement Gathering	ha harshpanghal	Feb 21 – 25	Medium	Medium	
✓ Designing	ha harshpanghal	Mar 3 – 10	High	Large	
✓ Implementation	ha harshpanghal	Mar 17 – Apr 25	High	Large	
✓ Testing	ha harshpanghal	May 1 – 10	Medium	Medium	
Add task...					

Task name	Assignee	Due date	Priority	Effort level	
✓ Implementation					
✓ Testing					
✓ <u>Deployment</u>					

- **Testing/characterization/interpretation/data validation:** Use tools such as JMeter, Selenium, or Postman to test your storage system's performance and functionality. Also, use data analytics tools such as Python, R, or Excel to interpret and validate data.



## CHAPTER 5

### CONCLUSION AND FUTURE WORK

#### **5.1. Conclusion.-**

- In this modern world the need for privacy and to protect this basic human right the blockchain based storage systems are the key to achieve that.
- User is able to sign for a account on meta mask and in doing so the keys are provided by hardhat. The photos are stored on pinata server on a decentralised network.
- The user feels more secure and it is fast and modernised according to the need of today's world and is scalable to all.
- It is accessible to all and conclusion to the months of hard work is a software application for storing and using

#### **5.2 Future work:**

- Our work can be extracted as app for users.
- Changes can be made to user interface.
- It can be made capable of uploading very large files.

## **References**

### **Reference Papers**

- [1] Gong, L.: San Francisco, CA (US) United States US 2003.01671.67A1 (12)  
PatentApplication Publication c (10) Pub. No.: US 2003/0167167 A1 Gong (43)  
Pub. Date: 4 September 2003 for Intelligent Virtual Assistant
  
- [2] Sarikaya, R.: The technology behind personal digital assistants. IEEE Signal  
Process. Mag.34,67–81 (2017)
  
- [3] Tsiao, J.C.-S., Tong, P.P., Chao, D.Y.: Natural-Language Voice-Activated  
PersonalAssistant, United States Patent (10), Patent No.: US 7,216,080 B2 (45), 8  
May 2007
  
- [4] AS Tulshan, SN Dhage - ... symposium on signal processing and intelligent ...,  
2018 – Springer
  
- [5] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using  
Blockchain to Protect Personal Data. In IEEE Security & Privacy Workshops.
  
- [6] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology  
Behind Bitcoin is Changing Money, Business, and the World. Penguin.
  
- [7] Underwood, S. (2016). Blockchain Beyond Bitcoin. Communications of the ACM,  
59(11), 15–17.
  
- [8] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and  
Application of the Next Internet Technology. Wiley.
  
- [9] Atzori, M. (2017). Blockchain Technology and Decentralized Governance: Is the  
State Still Necessary? Journal of Governance and Regulation, 6(1), 45–62.
  
- [10] Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain  
Applications. Springe

## **APPENDIX**

### **1. PLAGIARISM REPORT**